Domain Based Approach for QoS Provisioning in Mobile IP

Ki-Il Kim and Sang-Ha Kim

Department of Computer Science
220 Gung-dong ,Yuseong-gu, Chungnam National University, Deajeon 305-764, Korea
{kikim, shkim}@cclab.cnu.ac.kr

Abstract - **Mobile IP (MIP)[1] is proposed in order to ensure packet routing to the mobile host in the Internet regardless of the attachment point. MIP defines two new functional entities - Home Agent (HA) and Foreign Agent (FA) to manage the location of a mobile host. Also, MIP defines the tunneling mechanism to deliver packets that are destined to the mobile node's home address. But this tunneling mechanism has difficulties in adapting to Internet Service Architecture: Integrated Service (IntServ) and Differentiated Service (DiffServ). Since both services identify the service session as three-tuples - destinations IP address, IP protocol number and destination port - new different service session must be defined over IP tunnel. For that reason, how to guarantee the QoS over IP tunnel and map it to end-to-end service session are key features for MIP QoS. Therefore, current MIP QoS works are concentrating on this issue. However, current MIP QoS works seem to neglect the host mobility supporting protocol. Since MIP QoS is mostly dependent on the host mobility supporting protocol, we believe that the host mobility supporting protocol must be regarded as an important factor. The current host mobility supporting protocol has hierarchical architecture with micro mobility and macro mobility. So, if the MIP QoS can be organized as the same hierarchical architecture, the better QoS can be obtained. Since MIP can support host mobility in macro network, the IntServ and Diffserv must be applied in this section. However, since several schemes are proposed to support the fast handoff in micro level, the several QoS mechanism may be applied in this level. This paper specifics a hierarchical scheme, which uses not only aggregate RSVP flows between domain level agents, but also specific local policy between domain level agent and mobile host in a domain.**

I. Introduction

MIP is proposed in order to ensure packet routing to the mobile host regardless of the attachment point in the Internet. The efficiency of MIP is proved in small test-bed environments such as campus networks. The fundamental design goal of MIP is to minimize the frequency of route update as small as possible by introducing two new functional entities and tunneling mechanism between them. Therefore, MIP can support host mobility with minimized modification on routers except the access routers.

But, this tunneling mechanism may cause serious problems in adapting to the Internet QoS architecture – Integrated Service and Differentiated Service. Since both mechanisms identify the end-to-end service session by address field of IP header and port field of transport layer header, different sessions over tunneling section must be defined. Also, how to automatically map the new section over IP tunnel to the end-to-end service session must be defined.

In order to guarantee the QoS over IP tunnel section, three researches have been studied. All mechanisms mostly describe how to apply current QoS mechanism at the tunnel ingress point.

First, new RSVP session over IP tunneling section is created and is mapped to the end-to-end RSVP session using IntServ semantics [3][4]. Second, the edge router located on the tunneling entry point remarks the DSCP (Differentiated Service Code Points) in the IP header to reflect settled service level agreement [6]. In the third research, the entire RSVP requests are aggregated over tunneling.

But, the scalability problem also remains like RSVP in the first mechanism. That is, as the number of mobile host is increased, the session information per flow must be maintained. Also, since only qualitative QoS can be guaranteed in the second mechanism, quantitative QoS may not be guaranteed sometimes. Due to those reasons, the first two mechanisms cannot be implemented easily on the existing network too. Although the additional control message and state information is needed in the third mechanism when it is compared to the second mechanism, it is able to guarantee not only quantitative QoS but also qualitative QoS. Also, since flow aggregation makes the number of the state information small, the scalability problem can be removed. In order to guarantee end-to-end QoS, the suggested mechanism in this paper is based on the third mechanism.

The previous mechanisms seem to neglect the host mobility supporting protocol. Since the MIP QoS is mostly dependent on host mobility, it must be considered as one of the important factors. The host mobility supporting protocol is largely classified as two types – protocol supporting micro mobility and macro mobility. While the mechanism for macro mobility is converged to MIP, several other mechanisms have been proposed for micro mobility [8][9]. The classification is based on how often the handoff occurs.

Like the host mobility supporting protocol, the end-to-end QoS must be organized as macro level QoS and micro level QoS independently. Because the micro level QoS is mostly dependent on micro mobility supporting protocol, we do not mention it in this paper. Instead, we propose the macro level QoS guarantee mechanism. The domain level agents and aggregate RSVP signaling between them are defined for the macro level QoS.

This paper is organized as follows. The current MIP QoS trend is discussed in this section. In section II, we review the related works in detail. The suggested mechanism is presented in section III. In section VI and V, comparison with related works and simulation experiment are presented. The conclusion and future work are described in section VI.

II. Backgrounds

The current researches on MIP QoS are largely classified into two trends - how to guarantee QoS over a tunneling section and how to guarantee seamless real-time service regardless of handoff of a mobile host. In this section, we discuss how those issues are studied in the previous works briefly.

0-7803-7206-9/01/$17.00 © 2001 IEEE

The example mechanisms in QoS guarantee mechanisms over tunneling section between HA and FA are [3][4]. How to apply RSVP mechanism over IP tunneling is described in [3]. The tunneling section is defined as the new RSVP session from the tunnel ingress point to the egress point. Then, this RSVP session may be applied along the end-to-end path repeatedly. For RSVP session over a tunnel, Rentry (the tunneling entry point) must send an RSVP Path message and Rexit (the tunneling exit point) must reply with an RSVP Resv message. The newly created RSVP session over tunneling mentioned above is mapped with end-to-end RSVP session over non-tunneling on Rentry and Rexit points.

Also, the mechanism proposed in [4] specifies how to use RSVP as signaling for guaranteeing service quality in mobile environment. By introducing tunneling section in [3] between HA and FA, the mechanism proposed in [4] describes how to guarantee QoS and what scheme must be applied when the mobile host moves to another FA. The HA sends the new RSVP Path message to the FA in order to create the new RSVP session over IP tunnel when the periodical RSVP Update message arrived. This mechanism describes the case when the mobile host is a sender or a receiver separately.

The example of research for guaranteeing seamless real-time services is MRSVP[5]. In order to support real-time service by using IntServ architecture, MRSVP defines a new protocol, which is extended from the original RSVP. This extended protocol make it possible to guarantee real-time service quality though the mobile host moves continually. To minimize the effect of host mobility, MRSVP reserve resources in advance according to expected location, where mobile hosts is expected to move. To reserve resource in advance, MRSVP specifies the MSPEC. The MSPEC may be obtained by network or mobility profile of the mobile host itself.

In case of [4], the new RSVP session over the tunneling must be created or updated whenever the host moves. It may be a serious overhead in terms of implementation and scalability. The more the number of mobile hosts increases, the more RSVP sessions must be reserved in advance in [5]. This may make resource utilization low. Also how to predict information of the location, where mobile hosts may move, must be considered seriously. Also, both mechanisms neglect hierarchical host mobility to guarantee end-to-end QoS. Therefore, we propose a mechanism, which can solve the problem described through current Internet hierarchical architecture.

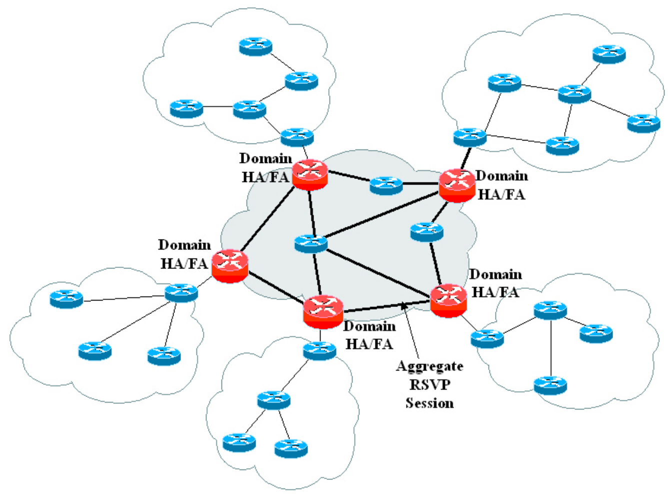
III. Hierarchical Mobile IP QoS Provisioning Mechanism

In this paper, the end-to-end QoS is defined as a combination of micro level QoS and macro level QoS. Since micro level QoS is mostly dependent on protocol supporting micro mobility, we do not consider it in this study. On the other hand, we propose a mechanism for macro level QoS guarantee. At this level, the protocol supporting host mobility is based on MIP.

Figure 1 shows an example configuration of architecture for the proposed mechanism. As shown in figure 1, the QoS from the domain agent to the host is defined as micro level QoS. The QoS between the domain agents is defined as macro level QoS. The domain agent has responsibility of supporting host mobility and perform the Call Admission Control (CAC). Also, CAC guarantees the service continuality of mobile host and controls data flow whether the QoS is guaranteed or not.

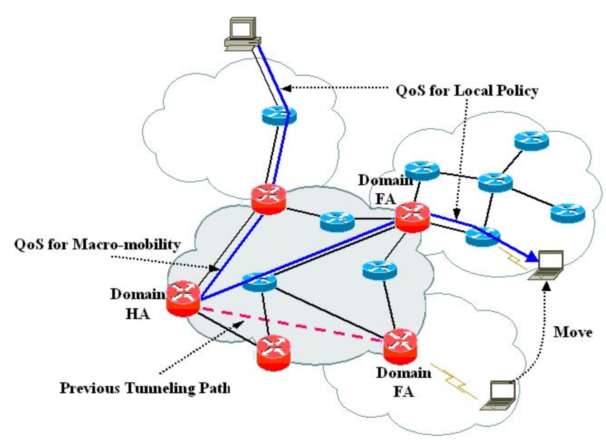
In order to introduce this mechanism into the current Internet, each gateway routers in one AS (Autonomous System) or domain must load HA/FA functionality independently. This agent performs the same functionality as domain root router in HAWAII and a cellular gateway router in Cellular IP in terms of mobility support.

Also, at least one aggregate RSVP session must be created between the gateway routers, which play the role of HA/FA. It means that the domain gateway is connected logically as a mesh form with each other. Therefore, one gateway router must maintain the state information as many as at least the number of border gateway routers. But, since the domain number is limited as a constant number, the scalability problem does not occur.



[Figure 1] The example configuration of architecture for the hierarchical MIP QoS provisioning

Under this architecture, the small flows, which come from the access network, must be mapped to several aggregate flows between gateways. That is, the domain agent performs the functionality of aggregating router or de-aggregating router. If traffic engineering is needed, aggregate tunneling flow in macro level may be implemented with RSVP–TE (RSVP–Traffic Engineering) and other mechanisms. The details on the traffic engineering subject remains as the future works.



[Figure 2] How to work when mobile host moves

In order to guarantee QoS for mobile hosts, each aggregated RSVP session between each domain level agent reserves more bandwidth (λ) than the bandwidth actually being used now for the further use. When mobile hosts move, previously reserved bandwidth (λ) is used for transmitting data of mobile host without reserving resource in macro level. Therefore, the service continuality can be maintained without any specific procedure for reserving bandwidth. Figure 2 shows the situation when a mobile host moves in other domains.

If mobile host moves to other domains as in figure 2, the micro level - from mobile host to domain FA - QoS is guaranteed by a specific policy, which is defined in protocol supporting micro mobility. But, the domain level - from domain level HA to domain level FA - QoS is guaranteed by previously reserved bandwidth.

Each HA checks periodically the bandwidth amount of λ. If λ is lower than the initial amount, the HA can detect that the new mobile host moves within its own domain and the previously reserved bandwidth is used. Then the HA sends the RSVP Path message to the FA in order to reserve the bandwidth as much as the currently used bandwidth + λ. This procedure is repeatedly accomplished to all aggregate RSVP session in the macro level. The FA, which has received the RSVP Path message, replies with the RSVP Resv message. The routers along the RSVP session path checks requirement of RSVP Resv message and reserves resources if possible. Through this procedure, the new aggregate RSVP session is created. Therefore, the reserved bandwidth is bounded by λ to the link capacity.

Variable	Description
bandwidth	Variable for the total bandwidth, which is expected to be reserved.
total_reserved_bandwidth	Reserved bandwidth amount between domain agents.
current_using_bandwidth	Being used bandwidth now for data transmission

[Table 1] Notation for Pseudo code

```
if (( total _reserved_bandwidth –current_using_bandwidth ) < λ )
{
      bandwidth = current_using_bandwidth + λ

      if  (( current_using_bandwidth + λ)  > link_capacity )
            send_aggregate_rsvp_path (FA,link_capacity)
      else
            send_aggregate_rsvp_path (FA,bandwidth)
else
      send_aggregate_rsvp_update (FA,bandwidth)
}
```

[Figure 3] Pseudo code for reserving the bandwidth

When the mobile host moves, the specific protocol is not used for guaranteeing QoS of a mobile host. For example, the HAWAII use Co-Care of Address (CcoA) for mobile host, it has the advantage of per flow management like RSVP. Also, bandwidth of aggregate RSVP session - from the old FA and HA - is reestablished as much as the currently used bandwidth + λ. Therefore, the reserved bandwidth in macro level is controlled flexibly by host's mobility. Since the aggregate RSVP session between the FA and HA is managed as the soft state, the update message must be sent to each FA periodically.

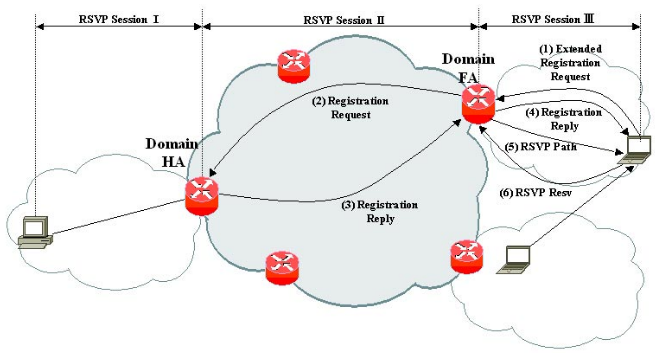
A. Applying the RSVP in micro level QoS

When the RSVP is applied in the micro level, the end-to-end RSVP session consists of several RSVP sessions. That is, three RSVP sessions - from the sender to HA, from HA to FA and from FA to mobile host - are used.

When the mobile host moves to another domain, the extended registration request message is sent to the domain FA. It includes the QoS requirements of each flow in mobile host. If the FA receives this message, it must send the original registration message, which is not extended to the domain HA. Next, the HA sends the registration reply message to the FA to confirm the registration. The FA relays it to the mobile host.

After registration is done successfully, the FA send an RSVP Path message to the mobile host based on information, which is included in extended registration request message. After the mobile host receives the RSVP Path message, the mobile host sends the RSVP Resv message to the FA.

When the mobile host moves within one domain, the extended registration message is sent to the FA. Then, FA does not send the registration request message to the HA as to the handoff within domain handoff. Meanwhile, the FA sends the RSVP Path message to the mobile host like handoff between domains. Figure 4 shows the example procedure when the RSVP is applied in macro level QoS. So, the effect of mobility is limited as the micro level QoS.



[Figure 4] The example of detail service provisioning

B. Applying the DiffServ in micro level QoS

When the DiffServ is applied in micro level QoS, the FA must decide the DSCP according to the QoS requirement received in the registration request message. The FA must perform the functionality of Bandwidth Broker (BB) in DiffServ. The DSCP is decided by the information, which is included in extended registration request message.

IV. FEATURE COMPARISON WITH PREVIOUS MECHANISMS

When the proposed mechanism is applied, each Internet Service Provider (ISP) has easier control on QoS policy in micro level by separating the micro level QoS and the macro level QoS than previous works.

Because the bandwidth is reserved for further use, the host mobility has little influence on the service continuality in our scheme. When the mobile host moves to other domains in [4], it is impossible to guarantee QoS while new RSVP session is created. Also, the proposed mechanism in [4] may guarantee the QoS from the HA to FA, but the QoS from a receiver to the sender may not meet the requirement. To achieve it, the reverse tunneling session must be created and maintained. However, although the different paths from the receiver to the sender are used in our scheme, the previously reserved bandwidth (λ) is used for transmitting the user data. It results from the assumption that the each domain agent has at least one aggregate RSVP. That is, two different aggregate RSVP sessions are maintained logically. Therefore, the reverse tunnel session is unnecessary.

The RSVP session in [4][5] is created and managed per flow. The management of all the sessions is a very difficult and a complex issue. Also, they may cause the scalability problems. The scalability problem can be solved by aggregated RSVP session as in our scheme.

	Simple QoS [4]	MRSVP [5]	Suggested Mechanism
Session management	Session management per flow	Session management per flow	Session management per aggregate flow
Reverse Tunneling	Required	Required	Not Required
Session creation when host moves	Required	Not Required	Not Required
Resource utilization	Very high	Very low resource utilization	Higher than [5] with aggregated flow
Service delay time	During creation of new service session	Very low	During creation of service session in the micro level

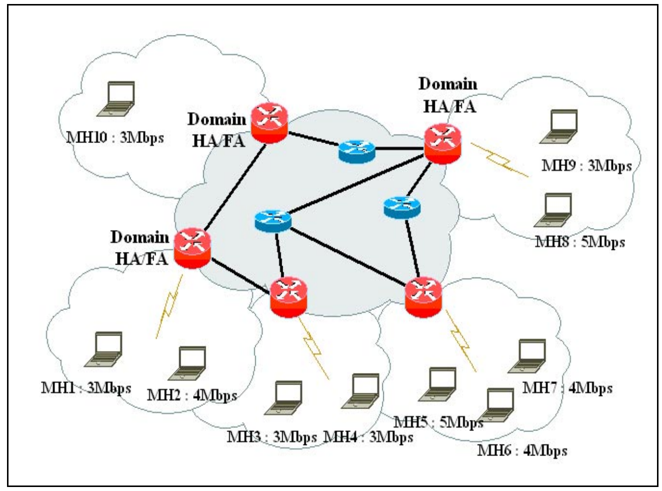
[Table 2] Feature comparison with other mechanisms

V. SIMULATION EXPERIMENT

In this section, we analyze the throughput of proposed mechanism through the simulation. The simulation is done with VINT (Virtual InterNetwork Testbed) Project – NS (Network Simulator). The parameter and topology for the simulation results are shown Table 3 and Figure 4, 5 and 6.

Traffic model	CBR (3Mbit/s: 5nodes, 4Mbit/s : 3 nodes, 5Mbits/s : 2 nodes)
Link capacity	10Mbit/s
Link delay	5ms
Queue size	50
Handoff time	Exponential distribution (Average time: 1 second)
Cell duration time	Exponential distribution (Average time: 20 second)
The gap of throughput measurement	1 second

[Table 3] Simulation parameters

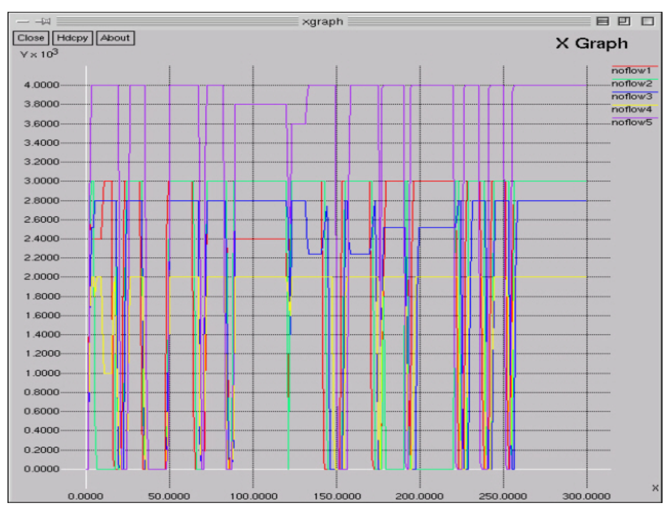


[Figure 5] Simulation topology

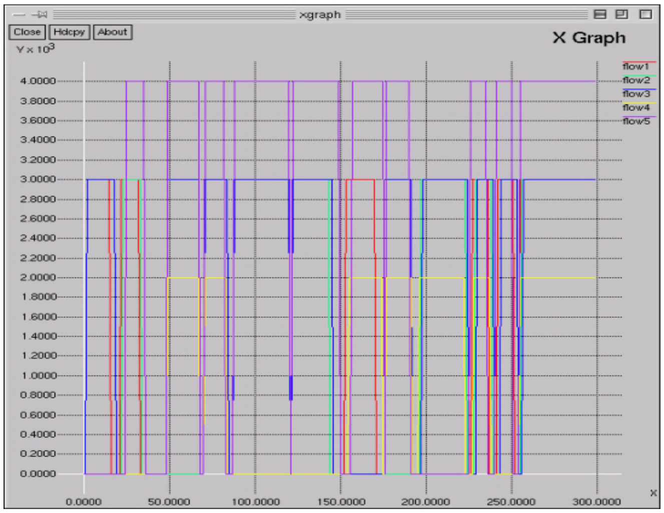
The aim of this simulation is to show that QoS can be guaranteed when each mobile host moves to each FA. The comparison mechanism is one proposed in [4] and in this paper. The flow1, flow4 and flow5 represent data reception rate when the suggested mechanism is applied. The flow1 shows data reception of 4Mbit/s and the flow4 shows that of 2Mbit/s and the flow5 shows that of 4Mbit/s. The delay_flow1, delay_flow4 and delay_flow5 represent data reception rate when mechanism in [4] is applied in the same order.

The figure 4 and 5 show the data rate of each receiver in uncontrolled flow and our scheme. The QoS is not guaranteed in uncontrolled flow. But, the line in figure 5 presents the data rate, which meets the requirements. The difference results from the fact the controlled flow controls the data flow in order to guarantee QoS of mobile host in connection.

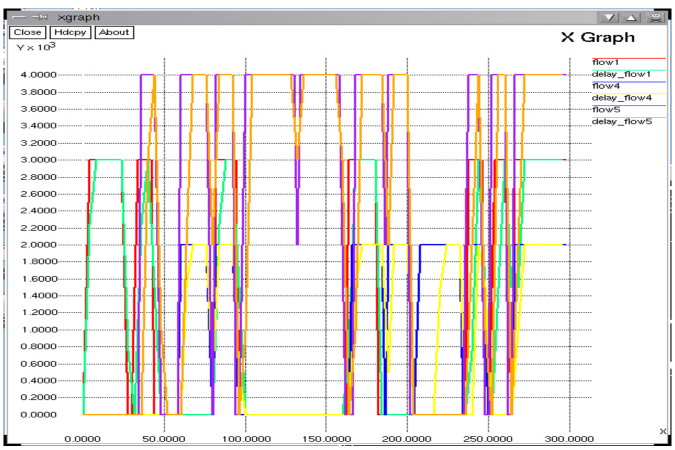
We can see that the mechanism proposed in [4] cannot guarantee the QoS requirement when the new RSVP session is created. But the suggested mechanism does not need the setup time of a new RSVP session when a mobile host moves.



[Figure 6] Uncontrolled flow



[Figure 7] Controlled flow by our mechanism



[Figure 8] The result of throughput measurement

VI. CONCLUSION AND FUTURE WORKS

In this paper, we propose a new scheme that guarantees the MIP QoS. We consider a hierarchical architecture that divides the macro level QoS and micro level QoS. The key feature of our scheme is the consideration of host mobility. Since the micro level QoS is dependent on the protocol supporting micro mobility, the micro level QoS guaranteeing mechanism is not mentioned here. We introduce domain level HA/FA and aggregated RSVP flow between each domain agent to support macro level QoS. The scalability problem can be solved by flow aggregation. Also, the quantitative QoS can be guaranteed by RSVP.

Related to this research, we will consider the inter-working with micro level QoS and how to apply this mechanism to the current the Internet. Also, the detailed implementation scheme remains as a future research object.

REFERENCES

[1] C.E.Perkins, "IP Mobility Support," RFC 2002, October 1996.
[2] J.D.Solomon, *Mobile IP : The Internet Unplugged*, PTR Prentice Hall, 1998.
[3] A.Terzis et al., "RSVP Operation Over IP Tunnels," RFC 2746, January 2000.
[4] A.Terzis et al., "A Simple QoS Signaling Protocol for Mobile Hosts in the Integrated Services Internet," Proceeding of the IEEE INFOCOM'99, vol. 3, March 1999, pp. 1011-1018.
[5] A.K.Talukdar et al., "MRSVP: A Reservation protocol for an Integrated Services Packet Networks with Mobile Hosts," Tech Report TR-337, Rutgers University.
[6] D.Black, "Differentiated Services and Tunnels," RFC 2983, October 2000.
[7] R.Ramjee et al., "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless Networks," ICNP '99.
[8] A.G.Valko, "Cellular IP : A New Approach to Internet Host Mobility," ACM Com. comm. Rev., 1999, pp. 50-65.
[9] Y. Bernet, *NETWORKING QUALITY OF SERVICE AND WINDOWS OPERATING SYSTEMS*, New Riders Publishing and Microsoft Corporate, 2001.